UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/799,371	03/12/2004	Bernard Kasser	00RO10154377	6357

27975 7590 11/07/2007

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
BAYOU, YONAS A	
ART UNIT	**PAPER NUMBER**
2134	

NOTIFICATION DATE	DELIVERY MODE
11/07/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/799,371	KASSER, BERNARD	
	Examiner	Art Unit	
	Yonas Bayou	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28 and 30-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28 and 30-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 09/26/2007.

2. Claims 1-28 and 30-34 are pending.

3. Claim 29 is cancelled.

4. Claims 1-28 and 30-34 are amended.

5. Applicant's arguments have been fully considered but they are not persuasive.

Response to Arguments

1. Applicant, on pages 20, 21 to page 22, line 14, of the remarks, argues "Chatani does not teach providing a user with a storage device storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers previously operated with the storage device; and determining possible fraudulent use of the storage device based upon the information list that is transmitted to the server, the server comparing the identification information in the information list with an authorized or fraudulent document reader list for determining fraudulent use of the storage device."

Examiner respectfully disagrees and asserts that Chatani discloses the memory card stores various firmware parameters and operating environment data that are specific to the particular network game console that the card is installed in. For

example, the memory card can be used to store the identification number (ID) assigned to the particular game console **[paragraph 24]**; and when the user makes a purchase, either through on-line or off-line means (e.g., telephone), a database record is maintained which records both the serial number of the playback machine and the serial number of the disk. If the user is ever forced to replace their playback machine, he or she could request a new unlock key by inserting the disk into the new playback machine. The database then confirms that the disk serial number shows a purchase against it and therefore allows a new unlock key to be generated for the user v**[paragraph 60]**. Once the user has received the unlock key, it can be entered into the playback machine through input means, such as a keyboard or some form of virtual keyboard. The playback machine stores the unlock key in a static memory area, such as a memory card or hard disk space. Upon execution, the main application program of the purchased software product verifies that the key is authentic and correct for that specific disk and playback machine. Assuming that the key is authentic, the main application is unlocked. For added security, the main executable file can be encrypted so that it cannot easily be hacked by an unauthorized user **[paragraph 63]**.

2. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-28 and 30-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Chatani et al., Pub. No. US 2002/0104019 A1 (hereinafter Chatani).

Referring to claims 1, 9, 17, 25 and 26, Chatani teaches a method which is inherently a method for securing circulation of an encrypted digital document to be reproduced with a document reader, the method comprising:

providing a user with a storage device (smart card) storing identification information identifying the storage device and for storing an identification information list comprising identification information identifying recent document readers previously operated the storage device **[page 3, paragraph 0024, lines 6-11 and fig. 1];**

transmitting to a server over a digital data transmission network from the storage device to the server upon connection of the storage device to the server by a terminal connected to the digital data transmission network and to the storage device

information identifying the digital document to be reproduced, and

the information list and the identification information of the storage device,**[page 2, paragraph 0017, lines 1-7 and page 7, paragraph 0058, lines 3-5]**;

identifying from the server the storage device on the basis of the information identification of the storage device transmitted to the server **[page 2, paragraph 0016, lines 3-6]**;

determining possible fraudulent use of the storage device based upon the information list that is transmitted to the server, the server comparing the identification information in the information list with an authorized or fraudulent document reader list for determining fraudulent use of the storage device **[page 8, paragraph 0060, lines 17-29 and paragraph 0063, lines 1-8]**;

if the storage device is not being fraudulently used, then transmitting over the digital data transmission network from the server to the computer terminal a decryption key specific to the digital document to be reproduced, with the decryption key being stored in the storage device **[page 8, paragraph 0063, lines 8-11]**;

decrypting the digital document using the stored decryption key by the document reader connected to the storage device **[page 4, paragraph 0032, lines 6-9**; and

reproducing the digital document decrypted by the document reader **[page 6, paragraph 0048, lines 11-14]**.

Referring to claims 2, 10, 18 and 27, Chatani teaches the method for secure distribution of digital document, wherein the decryption key is transmitted from the

storage device to the document reader only if the document reader is authorized **[page 6, paragraph 0045, lines 1-3 and page 6, paragraph 0048, lines 11-14].**

Referring to claims 3, 11, 19 and 28, Chatani teaches the method for secure distribution of digital document, wherein if the storage device is being fraudulently used, then the decryption key is not transmitted from the server to the storage device; and further comprising deactivating the storage device by the server for prohibiting further use of the storage device **[page 8, paragraph 0063;** inherently transmit the unlock key/decryption key from the server to the user if the user is unauthorized].

Referring to claims 4, 12, 20 and 30, Chatani teaches the method for secure distribution of digital document, wherein the information list also identifies unauthorized document readers; and wherein fraudulent use of the storage device is also determined if the identification information associated with the document reader is on the information list **[page 6, paragraph 0044, lines 1-4].**

Referring to claims 5, 13, 21 and 31, Chatani teaches the method for secure distribution of digital document, wherein the server builds from the identification information of the storage device and from the information list received from the storage device a table containing, for each identified document reader, a number of different storage devices used with the document reader; and further comprising:

determining that a particular document reader is unauthorized if the corresponding number of different storage devices used with this particular document reader exceeds a threshold **[page 1, paragraph 0006, lines 13-18]**; and

inserting the identification information of the document reader determined to be unauthorized into an unauthorized document reader list **[page 5, paragraph 0006, lines 17-24;** the authorized identification information stored in the memory card is inserted into the authorized Interactive Computer Entertainment System which is inherently inserted the unauthorized identification information of the document reader into an unauthorized document reader list].

Referring to claims 6, 14, 22 and 32, Chatani teaches the method for secure distribution of digital document, wherein if the storage device is being fraudulently used, then the decryption key is not transmitted over the digital data transmission network from the server to the storage device **[page 8, paragraph 0063;** inherently transmit the unlock key/decryption key from the server to the user if the user is authorized over a transmission network].

Referring to claims 7, 15, 23 and 33, Chatani teaches the method for secure distribution of digital document, wherein if the storage device is being fraudulently used, then the server deactivates the storage device over the digital data transmission network for prohibiting any further use of the storage device for reproducing a digital document **[page 7, paragraph 0058, lines 21-30;** if the storage device is not

fraudulent/authorized, inherently the identification information stored in the storage device has to be associated with the document reader so that it can be played/reproduced].

Referring to claims 8, 16, 24 and 34, Chatani teaches the method for secure distribution of digital document, wherein the decryption key specific to the digital document being reproduced is stored in the storage device in association with the information identifying the digital document to be reproduced; and wherein the document reader transmits to the storage device the information identifying the digital document that has been transmitted to it for reproducing, and then receives from the storage device the decryption key associated with the information identifying the digital document for decrypting the digital document **[page 4, paragraph 0032, lines 6-9 and page 6, paragraph 0048, lines 11-14]**.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Yonas Bayou

YB

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER